Recent is hier verandering in gekomen, en worden *ransomware* betalingen niet altijd meer gedekt door verzekeraars.[175]

Er is momenteel geen collectieve basis om organisaties te helpen hun weerbaarheid te vergroten. Elke organisatie moet zelf zijn basis opbouwen met de kennis en capaciteit die ze hebben.

Door de asymmetrische relatie tussen fabrikant en afnemer op het gebied van softwareveiligheid zijn afnemers doorgaans niet in staat zelf veiligheidseisen stellen bij de aanschaf van software en de juiste afwegingen maken. Er zijn wel mogelijkheden voor afnemers om bewust om te gaan met risico's van software, maar niet elke afnemer heeft de kennis en capaciteit om de juiste eisen te stellen en deze te controleren. Er bestaat geen algemene regelgeving omtrent de controle van software die fabrikanten verplicht aan bepaalde veiligheidseisen te voldoen.

Wat betreft preventie en voorbereiding op incidenten is er veel verschil in de weerbaarheid van organisaties. Veel maatregelen vergen een afweging van risico's. Niet alle organisaties hebben de expertise en capaciteit om maatregelen voldoende uit te voeren, of onderkennen de urgentie om hier capaciteit op in te zetten niet. Iedere organisatie is zelf verantwoordelijk voor zijn digitale weerbaarheid. Er is geen collectief fundament dat geboden wordt om organisaties te helpen de digitale weerbaarheid te vergroten.

4.3 Incidentbestrijding (respons)

De voorvallen die we in hoofdstuk 3 beschrijven laten zien dat de tijd tussen dat een kwetsbaarheid in software wordt gemeld en dat organisaties die kwetsbaar zijn worden aangevallen beperkt is: variërend van een maand tot enkele dagen of geen (*zero day*). In de vorige paragrafen beschreven we welke factoren van invloed zijn op de wijze waarop fabrikanten kwetsbaarheden in software voorkomen en reageren op kwetsbaarheden en wat organisaties die software gebruiken doen om te voorkomen dat hun digitale systeem daardoor beveiligingslekken kan hebben. In deze paragraaf gaan we in op de factoren die beïnvloeden hoe betrokken partijen, zoals fabrikant, organisatie en publieke en private incidentbestrijders het incident bestrijden om de gevolgen te beperken.

4.3.1 Informatiestroom

Na het bekend worden van een kwetsbaarheid is van cruciaal belang dat de relevante organisaties zo direct en zo snel mogelijk worden geïnformeerd. Organisaties die de software gebruiken hebben zo betrouwbaar en toegesneden mogelijke informatie nodig om in korte tijd een eigen afweging te maken hoe te handelen om de risico's te kunnen beheersen. Organisaties die niet in staat zijn om een eigen afweging te maken hebben behoefte aan een advies dat ze kunnen volgen. Fabrikanten en incidentbestrijders willen

175 Verzekeraars deinzen terug voor ransomware', *AG Connect*, https://www.agconnect.nl/artikel/verzekeraars-deinzen-terug-voor-ransomware, 25 mei 2021.

weten hoe veel en welke organisaties kwetsbaar zijn en op welke manier deze worden aangevallen, zodat zij de juiste maatregelen kunnen nemen, faciliteren en/of adviseren. Deze informatie kan via een veelheid aan bronnen worden verzameld, zoals fabrikanten, vrijwillige en commerciële beveiligingsonderzoekers, CERTS via *coordinated vulnerability disclosure-procedures* en inlichtingen- en veiligheidsdiensten. De in dit rapport onderzochte voorvallen laten zien dat er op dit moment belemmeringen zijn om ervoor te zorgen dat informatie die vanuit verschillende publieke en private bronnen binnenkomt, zo snel mogelijk alle organisaties bereikt die deze informatie nodig hebben om de gevolgen van kwetsbaarheden in software te bestrijden.

Belemmeringen in het delen van informatie

Informatievoorziening is van cruciaal belang voor organisaties, omdat snel reageren bij incidenten als in dit onderzoek noodzakelijk is om binnendringen te kunnen voorkomen.[176] De meeste landen hebben een nationale autoriteit die optreedt als incidentbestrijder. In Nederland is NCSC het nationale CERT. De positie van nationale CERT is onder meer relevant, omdat andere partijen zoals softwarefabrikanten per land het nationale CERT gebruiken als aanspreekpunt, bijvoorbeeld om door te geven welke organisaties in een bepaald land kwetsbaar zijn om te worden aangevallen.

Bij het delen van informatie staan twee soorten informatie centraal: voorlichtingsinformatie (om te komen tot een handelingsperspectief of berichten over kwetsbaarheden en beveiligingsadviezen) en dreigingsinformatie. Dreigingsinformatie bestaat uit aanvallers-informatie en slachtofferinformatie. De knelpunten tijdens de incidentbestrijding hebben vooral betrekking op dreigingsinformatie: informatie over welke organisaties kwetsbaar zijn en hoe de aanvallers kunnen worden herkend.[177] Daarbij gaat het met name om de slachtofferinformatie die niet wordt gebruikt, waardoor partijen niet worden gewaarschuwd.

Bij NCSC komt veel informatie samen uit verschillende bronnen: naast fabrikanten gaat het om inlichtingen- en veiligheidsdiensten, andere overheden, sectorale samenwerkingsverbanden (ISAC's), onafhankelijke beveiligingsonderzoekers (al dan niet via DIVD), cybersecurity bedrijven en IT-dienstverleners, evenals berichten op social media zoals Twitter, Reddit en vakmedia. Geïnterviewde organisaties gaven aan momenteel zelf via formele en informele bronnen informatie te zoeken, omdat ze de gewenste informatie via NCSC niet of te laat krijgen.

Waargenomen juridische belemmeringen

NCSC stelt vast dat zij vanuit hun wettelijk gelimiteerde mandaat en andere juridische belemmeringen zoals de AVG beperkt is in het delen van slachtofferinformatie (zoals IP-adressen van kwetsbare servers) met organisaties die deze nodig hebben, namelijk dat zij deze informatie alleen mag delen met rijksoverheid en vitale aanbieders.[178] Tijdens de Citrix-crisis heeft het NCSC besloten om af te wijken van de eigen wettelijke kaders en dreigingsinformatie te delen met een aantal schakelorganisaties zoals Z-CERT en de IBD,

176 Dit belang is onlangs onderstreept in het adviesrapport *Integrale aanpak cyberweerbaarheid* van de Cyber Security Raad (april 2021).
177 Definitie Dialogic en TU/e (2020).
178 Het wettelijk mandaat van NCSC is geregeld in de Wet beveiliging netwerk- en informatiesystemen (Wbni), die sinds 9 november 2018 van kracht is.

in navolging daarvan zijn deze kaders in 2020 en 2021 verbreed. Overige sectoren waaronder vrijwel het gehele Nederlandse bedrijfsleven (1,8 miljoen bedrijven[179]) kregen geen dreigingsinformatie.

Een volgende belemmering is gelegen in *welke* informatie NCSC deelt met de informatieknooppunten. NCSC stelt zich namelijk op het standpunt dat het volgens de Wbni vertrouwelijke, tot aanbieders herleidbare gegevens alleen mag delen met CERTs, CSIRTs en inlichtingendiensten, en niet met OKTT's. Het ministerie van JenV beschouwt IP-adressen van kwetsbare servers als dergelijke vertrouwelijke, tot aanbieders herleidbare gegevens in het kader van de Wbni en als persoonsgegevens in het kader van de AVG.

In een onderzoek naar informatiedeling in opdracht van het WODC wordt erkend dat de institutionele setting en wet- en regelgeving belemmeringen opwerpen voor NCSC om informatie te kunnen delen, maar geeft aan dat deze belemmeringen mede het gevolg zijn van de wijze waarop het ministerie van JenV de regels interpreteert. Met andere woorden, het is binnen de huidige kaders van de wet- en regelgeving ook mogelijk om tot andere juridische inzichten en een ander oordeel te komen en tot het besluit om de informatie wel te delen.

In het onderzoek van WODC wordt geen uitspraak gedaan over wat de juiste visie is, wel dat het belangrijk is dat er consensus komt op dit punt. Daarom bevelen de onderzoekers aan dat er vervolgonderzoek wordt gedaan op deze juridische vragen. De minister van JenV kondigde een voorstel voor wetswijziging aan die de belemmering moet wegnemen door de bevoegdheden van het NCSC om relevante dreigingsinformatie te delen te verruimen. Het kan echter één tot enkele jaren duren voor deze wet is aangenomen en wordt uitgevoerd.[180]

De incidentbestrijding in Nederland, waaronder het verzamelen en delen van informatie, is gefragmenteerd en bevat hiaten. Daardoor is voor veel organisaties, waaronder een groot deel van het Nederlandse bedrijfsleven, niet geregeld dat zij tijdig informatie ontvangen wanneer zij gevaar lopen. Het gaat daarbij in het bijzonder om slachtofferinformatie, oftewel dat een organisatie (ook ongevraagd) wordt gewaarschuwd dat zijn systemen kwetsbaar zijn en hij risico loopt om te worden aangevallen. Het NCSC, dat op dit moment ten behoeve van heel Nederland de informatie ontvangt vanuit onder meer fabrikanten, NCSC's in andere landen, inlichtingen- en veiligheidsdiensten en andere gremia, deelt deze slachtoffer-informatie nu alleen met een selecte groep organisaties, maar niet met decentrale overheden en het merendeel van het Nederlandse bedrijfsleven en vanuit het uitgangspunt dat een organisatie vooraf toestemming geeft om te worden geïnformeerd.

179 ZZP, MKB en bedrijven. Bron: https://www.digitaltrustcenter.nl/over-het-digital-trust-center
180 Dialogic en TU/e, *Informatie-uitwisseling landelijk dekkend stelsel cybersecurity* in opdracht van WODC, 14 oktober 2020. https://www.rijksoverheid.nl/actueel/nieuws/2021/06/28/meer-mogelijkheden-ncsc-en-dtc-om-dreigings--en-incidentinformatie-te-delen

Inrichting middels Landelijk Dekkend Stelsel

Om de mogelijkheden voor informatiedeling te verbeteren werkt de minister van JenV aan een Landelijk Dekkend Stelsel van samenwerkingsverbanden op het gebied van cybersecurity[181], zodat NCSC informatie mag delen met organisaties die aangewezen worden om deze informatie te mogen ontvangen en doorgeven. Dit levert een stelsel op met een groot aantal organisaties die elk een apart loket vormen voor hun achterban en ook onderling informatie aan elkaar doorgeven. In een dergelijk stelsel treedt vertraging op doordat het tijd kost om uit te zoeken voor welk informatieknooppunt bepaalde informatie relevant is. En bij elke tussenstap kan informatie verloren gaan. Het NCSC als nationale CERT verliest daardoor kostbare tijd, waardoor ze niet in staat is adequaat de overheidsrol binnen de digitale sector te faciliteren. Naast het Landelijk Dekkend Stelsel van schakelorganisaties is het informele circuit, bestaande uit vrijwilligers, ook van belang om de snelheid in de informatiedeling te behouden.

Een andere belemmering is dat niet alle organisaties in Nederland in het Landelijk Dekkend Stelsel worden 'afgedekt' door samenwerkingsverbanden op het gebied van cybersecurity, met name het bedrijfsleven vormt een witte vlek. Daar zitten bedrijven bij die een belangrijke functie vervullen voor vitale aanbieders, of voor andere maatschappelijk belangrijke organisaties die niet onder de definitie vitaal vallen, zoals de voedselsector. Om die reden kondigde de minister van JenV een wetsvoorstel aan waarin onder meer zou worden geregeld dat NCSC via DTC informatie kon delen met het Nederlandse bedrijfsleven ('de rest van de rest').[182] Daarnaast heeft het ministerie van EZK een wetsvoorstel aangekondigd om de wettelijke basis van het DTC te versterken. Op basis daarvan start DTC in het najaar van 2021 een proef om met 40 bedrijven die zich daarvoor aanmelden dreigingsinformatie te delen.[183]

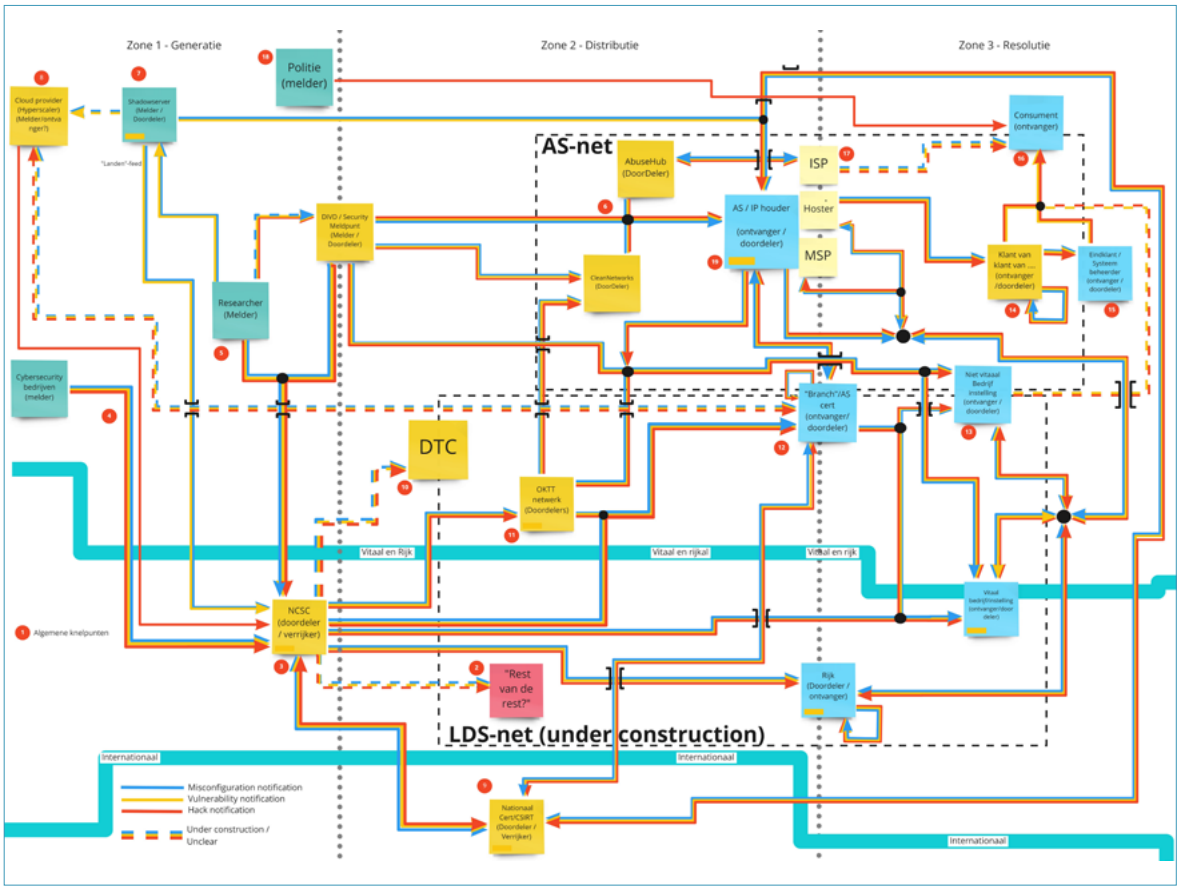
Met deze inspanningen wordt het stelsel meer 'dekkend', maar de informatiedeling blijft versnipperd over een groot aantal schakelorganisaties, die elk capaciteit en expertise moeten inzetten om op een zinvolle manier met de informatie om te kunnen gaan. De volgende figuur die het Anti Abuse Netwerk (AAN) maakte van de wijze waarop dreigingsinformatie tussen organisaties wordt uitgewisseld, maakt duidelijk hoe gecompliceerd de informatiedeling is.[184]

181 NCSC noemt dit schakelorganisaties. https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds

182 https://www.rijksoverheid.nl/actueel/nieuws/2021/06/28/meer-mogelijkheden-ncsc-en-dtc-om-dreigings--en-incidentinformatie-te-delen

183 https://www.rijksoverheid.nl/ministeries/ministerie-van-economische-zaken-en-klimaat/nieuws/2021/09/13/digital-trust-center-start-met-actief-informeren-bedrijven-over-digitale-dreigingen

184 Zo bestaat DTC op dit moment uit 20 fte om een achterban van 1,8 miljoen bedrijven te bedienen en heeft DTC geen rechtstreekse relatie met deze bedrijven, alleen via samenwerkingsverbanden (extra schakels in de informatiedeling).



Figuur 18: Metrokaart van de uitwisseling van dreigingsinformatie over organisaties. (Bron: AAN)[185]

Tenslotte hebben belemmeringen om informatie te delen tussen lidstaten en tussen private en publieke entiteiten een negatieve invloed op de effectiviteit van cybersecuritymaatregelen en het beeld van de omvang en ernst van de situatie.[186]

Belemmeringen in het verzamelen van informatie

Een ander vraagstuk is of NCSC en de andere informatieknooppunten zelf informatie mogen vergaren die nodig is om organisaties te helpen de gevolgen te bestrijden. De voorvallen die we in dit onderzoek analyseren tonen dat IP-adressen van kwetsbare servers cruciaal zijn om organisaties te overtuigen van de urgentie om in te grijpen en belangrijke sturingsinformatie is om een beeld te vormen van de situatie en de mate waarin deze onder controle is (zie verder 4.3.2).

Via bepaalde tools op het internet kunnen onderzoekers de buitenkant van digitale systemen scannen en op deze manier in kaart brengen welke servers gebruik maken van een bepaalde versie van bepaalde software. Deze manier van scannen maakt niet zichtbaar of deze servers nog kwetsbaar zijn (of de organisatie de mitigerende maatregel of patch al heeft uitgevoerd). Om dat zichtbaar te maken, wordt doorgaans een scan uitgevoerd, waarmee degene die scant als het ware 'aan de deur voelt' om te kijken of deze op slot zit of geopend kan worden. Dergelijke scans worden in de praktijk veel

185 https://www.abuse.nl/publicaties/metrokaart-december-2020.html
186 European Parliament, *The NIS2 Directive – A high common level of cybersecurity in the EU*, 2021. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

uitgevoerd en in sommige gevallen ook aangeraden door fabrikanten en nationale CERTs.[187]

Binnen NCSC is behoefte om in ieder geval te kunnen scannen om in kaart te brengen op welke servers bepaalde software in gebruik is en bij voorkeur ook of deze servers nog kwetsbaar zijn, om op deze manier gerichter te kunnen waarschuwen en een beter beeld te krijgen van de omvang van de situatie. Juristen binnen NCTV ontraden dit echter vanwege de juridische risico's die ze daarin zien. Zo worden de scantools ook gebruikt door aanvallers en vrezen zij dat het 'aan de deur voelen tot computervredebreuk leidt.[188]

De voorvallen die in hoofdstuk 3 zijn beschreven laten zien dat vrijwillige beveiligingsonderzoekers, onder andere vertegenwoordigd in het DIVD, dit hiaat in de informatievoorziening en incidentbestrijding proberen op te vullen, door te scannen welke organisaties kwetsbare systemen hebben en deze organisaties te waarschuwen. Ook NCSC en andere CERTs maken van hun informatie gebruik. Dit is echter een kwetsbare situatie. Deze beveiligingsonderzoekers doen dit vrijwillig, meestal naast een fulltime baan. Vanwege het grote aantal kwetsbaarheden en aanvallen de laatste tijd heeft dit een enorme belasting opgeleverd voor deze vrijwilligers.[189]

Situatie verschilt per organisatie

De versnippering en witte vlekken in het landschap van informatieknooppunten zorgt er niet alleen voor dat relevante informatie betreffende organisaties niet bereikt, maar ook dat het niet mogelijk is om een consistent beeld te vormen van de omvang en ernst van een voorval. Elke (overheids)organisatie dient zelf een impactanalyse te maken en zelf een afweging te maken of zij adviezen van de informatieknooppunten of samenwerkingsverband waarbij ze zijn aangesloten wel of niet opvolgen en welke acties zij ondernemen. Zowel het uit voorzorg uitzetten als het aan laten staan kan gevolgen hebben voor de digitale veiligheid, maar deze risico's en de perceptie daarvan verschillen per organisatie.

Het gevolg is dat sommige organisaties direct maatregelen nemen bij een incident, en andere dat niet kunnen of niet willen (zie paragraaf 4.2 voor nadere analyse van de afwegingen die organisaties maken). Organisaties bleken in de praktijk meestal niet terug te koppelen hoe ze met de adviezen om zijn gegaan, waardoor bij deze informatieknooppunten een diffuus beeld ontstond van de mate waarin de situatie in Nederland onder controle is. Daar kwam bij dat als een organisatie geen maatregelen neemt, dit niet alleen een risico kan opleveren voor de organisatie zelf, maar ook voor de ketenpartners van deze organisatie (leveranciers en klanten).

187 Zie bijvoorbeeld https://www.us-cert.gov/ncas/alerts/aa20-031a. In het geval van de Citrix-kwetsbaarheid wordt tijdens de scan een niet-bestaand bestand opgevraagd op de Citrix-server op een locatie waar de gebruiker geen toegang toe zou moeten krijgen. Als de Citrix-server antwoordt dat het bestand niet bestaat, is duidelijk dat de kwetsbaarheid nog op de server aanwezig is.

188 Niet-openbare bron: memo's en mailwisseling.

189 Zie bijvoorbeeld deze podcast waarin DIVD-ers vertellen over hun betrokkenheid bij het Kaseya voorval. https://www.cyberhelden.nl/episodes/episode-27/, juli 2021.

De Rijksoverheid streeft er naar dat de informatie die NCSC wel wil delen beter wordt uitgewisseld via het zogenoemde Landelijk Dekkend Stelsel, waarin sectorale organisaties en (groepen) bedrijven ook op vrijwillige basis informatie met elkaar delen die cruciaal is voor het bestrijden van incidenten. Echter als het NCSC als nationaal aanspreekpunt informatie wel ontvangt maar niet volledig deelt, worden ook bij een volledig dekkend stelsel niet alle potentiële slachtoffers gewaarschuwd. Beveiligingsonderzoekers proberen dit hiaat op te vangen, door – op vrijwillige basis – het Nederlandse internetdomein te scannen op kwetsbare servers en deze informatie te delen met partijen die kunnen waarschuwen. Dat is echter een kwetsbare situatie omdat zij hierin niet werden gefaciliteerd: noch door de overheid, noch door andere betrokken partijen, waardoor hun structurele inzet niet is geborgd.[190]

4.3.2 Ontwikkelingen in de incidentbestrijding

Wat de voorvallen tonen is dat goede samenwerking tussen overheid en organisaties is cruciaal is om incidenten te bestrijden. En om ze te voorkomen (zie paragraaf 4.1 en 4.2). Onderling vertrouwen is cruciaal om dit tot stand te brengen, evenals een consistente nationale aanpak.[191]

In een aantal andere landen zijn het cybersecuritystelsel en de incidentbestrijding centraal ingericht, ook in Nederland klinkt de roep om meer centrale aansturing. In Nederland is gekozen voor decentrale aansturing in de incidentbestrijding. Decentrale aansturing zou passen bij de Nederlandse cultuur. Centrale aansturing van cybersecurity en incidentbestrijding in andere landen (zie kader) gaat vaak gepaard met regie vanuit inlichtingendiensten. In Nederland zou centrale aansturing daarom weerstand kunnen oproepen.[192]

190 Inmiddels is deze situatie veranderd: eind september 2021 kondigde het bedrijfsleven aan om zelf een waarschuwingssysteem op te zetten. Bron: *FD*, Bedrijfsleven start eigen alarmsysteem tegen hackers: 'overheid te traag', 28 september 2021.

191 Atkins, S. en C. Lawson, An Improvised Patchwork: Success and Failure in *Cybersecurity Policy for Critical Infrastructure. Public Administration Review*, Vol. 81, Iss. 5, pp. 847–861, 2020.

192 Zie onder andere: Rand, *Cybersecurity A State-of-the-art Review Phase 2: Final Report*, 2020. NSOB, *Actuele kwestie, klassieke afweging. Een verkenning naar de governance van het Nederlands digitaliseringsbeleid*, 2021.

Incidentbestrijding in andere landen

Het Britse NCSC is de centrale organisatie voor cybersecurity in het Verenigd Koninkrijk. Naast het bestrijden van incidenten zijn zij ook een expertisecentrum en helpen zij om de digitale weerbaarheid van zowel overheid als bedrijfsleven te vergroten. Dit NCSC valt onder de Britse inlichtingendienst GCHQ en heeft daardoor toegang tot hoogstaande expertise en inlichtingen. Het cybersecurity beleid wordt gemaakt door de *Cabinet Office*, dus op het niveau van de regering (departement overstijgend). In Frankrijk lijkt het GIP ACYMA (vergelijkbaar met DTC) goed te zijn om kleine bedrijven te bereiken door ze te koppelen aan private IT experts. En in Duitsland is de incidentbestrijding net als in Nederland versplinterd, onder meer vanwege het federale bestuurssysteem.[193]

Het Amerikaanse *Cybersecurity and Infrastructure Security Agency* (CISA) is net als het Britse NCSC zowel gericht op incidentbestrijding als verbetering van de weerbaarheid voor alle overheidsorganisaties en bedrijven in de VS. Ze werken nauw samen met de private sector en brengen regelmatig adviezen uit in samenwerking met de NSA en FBI.[194]

Naar aanleiding van evaluaties en kamerbrieven die over de voorvallen zijn verschenen, zijn en worden maatregelen genomen om de incidentbestrijding te verbeteren, zoals het wetsvoorstel van de minister van JenV dat mogelijk moet maken om meer informatie te delen met partijen die niet tot de doelgroep van Rijk en vitaal behoren. Ook worden gemeenten aangesloten op het Nationale Detectie Netwerk, dat voorheen, met in achtneming van de Wbni, was voorbehouden aan rijk en vitaal. Hieruit blijkt dat de rijksoverheid dit onderscheid weliswaar wettelijk nog handhaaft, maar in de praktijk langzaamaan loslaat. Daarbij blijft de informatiedeling echter plaatsvinden binnen de kaders van de decentrale aansturing. Uit de analyse van de voorvallen blijkt dat als sprake is van een kwetsbaarheid die wereldwijd wordt aangevallen, de tijd om te reageren beperkt is tot enkele dagen of helemaal geen (*zero day*). Decentrale aansturing leidt tot verlies van tijd en informatie, waardoor organisaties niet tijdig worden geïnformeerd dat zij gevaar lopen.

Een andere ontwikkeling die uit de analyse van de voorvallen blijkt, is dat vanuit de Rijksoverheid (JenV, BZK) politiek-bestuurlijk behoefte is gebleken om te kunnen verantwoorden dat alle relevante organisaties in Nederland de adviezen van NCSC opvolgen. Daarbij gaat het niet alleen om organisaties die vallen onder het mandaat van NCSC, maar ook organisaties daarbuiten zoals gemeenten, provincies en zorginstellingen. Hieruit kan worden afgeleid dat er behoefte is aan centrale sturing, die nu niet bestaat. Omgekeerd voelden deze organisaties door het ongerichte advies van NCSC en de soms directe contacten vanuit het rijk druk om adviezen op te volgen, terwijl er formeel geen sturings- en verantwoordingsrelatie bestaat met het Rijk. Deze organisaties hebben eigen gremia die hen aanstuurt en waaraan ze verantwoording afleggen.

193 Dialogic en TU/e, *Informatie-uitwisseling landelijk dekkend stelsel cybersecurity* in opdracht van WODC, 14 oktober 2020.
194 https://www.cisa.gov/